JOURNAL OF ALGEBRA 169, 418–440 (1994)

R-Hopf Algebra Orders in KC_{p^2}

ROBERT G. UNDERWOOD*

Department of Mathematics, Auburn University at Montgomery, Montgomery, Alabama 36117-3596

Communicated by Susan Montgomery

Received January 16, 1993

INTRODUCTION

Let K be a finite extension of the p-adic rationals Q_p and let ν denote the p-adic valuation on K with $\nu(p) = 1$. Let R denote the integral closure of Z_p in K. If G is a finite abstract group, then the group ring KG can be endowed with the structure of a K-Hopf algebra. An R-Hopf algebra order in KG is an R-Hopf algebra H which is a finitely generated, projective R-module satisfying

$$H \otimes_R K \cong KG$$

as K-Hopf algebras. R-Hopf algebra orders in KG play an important role in the representation theory of the finite group G, see [L3, L4]. In addition, R-Hopf algebra orders in KG can be used to describe the ring of integers of Galois extensions L/K with abelian Galois group G, see [C and G]. For these reasons it is important to determine the structure of R-Hopf algebra orders in KG. For G cyclic of order p, Tate and Oort have given a complete classification of R-Hopf algebra orders in KG, see [TO]. The structure of R-Hopf algebra orders in KC_{p^2}, where C_{p^2} denotes the cyclic group of order p^2, has been under investigation by Larson in [L2, L3] and by Greither in [G]. Larson [L3] has shown that order bounded group valuations on C_{p^2} give rise to R-Hopf orders in KC_{p^2}, which we call *Larson orders*. Greither in [G] obtains a large class of R-Hopf orders in KC_{p^2} by computing the representing algebras of a certain collection of R-group schemes of order p^2. We will refer to these R-Hopf orders as *Greither orders*. To my knowledge, there is no known classification of R-Hopf orders in KC_{p^2}, so in this paper we prove the following theorem.

MAIN THEOREM. *Let H be an R-Hopf algebra order in KC_{p^2}. Then H is either a Greither order or its linear dual H^* is a Greither order.*

*The author is indebted to the referee for the numerous suggestions and comments which improved this paper considerably.

0021-8693/94 $6.00
Copyright © 1994 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Hence, in this manner we obtain a complete classification of R-Hopf algebra orders in KC_{p^2}.

It has been convenient to organize this paper into two parts. In Part 1, we give definitions and survey some basic results on R-Hopf orders. This leads to Part 2, in which we state and prove the major theorems, including the main theorem.

1

1.0. *Hopf Algebra Preliminaries*

In this section, we discuss the basic properties of R-Hopf algebra orders in KC_{p^2}. We have that K is a finite extension of Q_p, endowed with the p-adic valuation ν. We set $\nu(p) = 1$. We assume throughout this paper that K contains a primitive p^2-nd root of unity, denoted ζ. Note that $\nu(1 - \zeta) = 1/p(p - 1)$ and $\nu(1 - \zeta^p) = 1/(p - 1)$. The integral closure of Z_p in K, denoted R, is a local ring with maximal ideal m. In terms of ν,

$$R = \{x \in K | \nu(x) \geq 0\}$$
$$m = \{x \in R | \nu(x) > 0\}$$
$$U(R) = \{x \in R | \nu(x) = 0\},$$

where $U(R)$ denotes the units group of R.

For the purposes of this paper, all algebras over R are assumed to be commutative. We will denote the diagonal, counit, and antipode maps of the R-Hopf algebra H by Δ_H, ε_H, and σ_H, respectively.

Let KC_{p^2} be the group ring of the cyclic group of order p^2. *An R-Hopf algebra order in KC_{p^2}* is an R-Hopf algebra H which is finitely generated and projective as an R-module and which satisfies $H \otimes_R K \cong KG$ as K-Hopf algebras.

The group ring RC_{p^2} is an R-Hopf algebra order in KC_{p^2} via the maps $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$, $\sigma(g) = g^{-1}$, with $C_{p^2} = \langle g \rangle$. If H is an R-Hopf order in KC_{p^2}, then Larson has shown that $RC_{p^2} \subseteq H$ (see [L5]).

Since $\zeta \in K$, $H^* = \mathrm{Hom}_R(H, R)$ is an R-Hopf order in $K\bar{C}_{p^2} \cong KC_{p^2}$, where $\bar{C}_{p^2}$ denotes the cyclic group of characters. It can be shown that if A and B are two R-Hopf orders, then $A \subseteq B$ iff $B^* \subseteq A^*$ (for a proof see [U, Sect. 1.1]).

As an R-algebra, the dual $RC_{p^2}^*$ can be written

$$RC_{p^2}^* = \bigoplus_{i=0}^{p^2-1} \mathrm{Re}_i$$

with idempotents $e_i = (1/p^2)\sum_{j=0}^{p^2-1}\zeta^{-ij}\chi^j$, where $\chi^j(g^i) = \zeta^{ij}$. Now if H is any R-Hopf order in KC_{p^2}, the identification $g \mapsto \chi$ induces an inclusion $H \subseteq RC_{p^2}^*$, hence $RC_{p^2}^*$ is referred to as the *maximal integral order* in KC_{p^2}.

The *space of left integrals* of an R-Hopf order H in KC_{p^2} is defined to be the set

$$L_H = \{\Lambda \in H | h\Lambda = \varepsilon_H(h)\Lambda\} \qquad \text{for all } h \in H.$$

If $\Lambda \in L_H$ is such that $L_H = R\Lambda$, then Λ is called a *generating integral* for H. Since R is a PID, every R-Hopf order has a generating integral. For example, the element p^2e_0 is a generating integral for the Hopf order RC_{p^2}. Note that the ideal $\varepsilon_H(L_H)$ in R is principal and generated by $\varepsilon_H(\Lambda)$, where Λ is a generating integral. For example, when $H = RC_{p^2}$, we find that $\varepsilon_{RC_{p^2}}(L_{RC_{p^2}}) = p^2R$.

1.1. *Larson Orders*

For $n \geq 1$, Larson [L3] gives a method for constructing R-Hopf algebra orders in KC_{p^n} using order bounded group valuations. A *group valuation* on $C_{p^n} = \langle g \rangle$ is a function $\xi\colon C_{p^n} \to Q \cup \infty$ satisfying

(1) $\xi(1) = \infty$

(2) $0 \leq \xi(g^i) < \infty$, for $i = 1, \ldots, p^n - 1$

(3) $\xi(g^i) = \xi(g^{-i})$, for all i

(4) $\xi(g^ig^j) \geq \min\{\xi(g^i), \xi(g^j)\}$, for $i, j = 0, \ldots, p^n - 1$.

Let ξ be a group valuation on C_{p^n}. If the range of ξ is contained in the range of ν, then ξ is an *order bounded* group valuation (o.b.g.v.) if

$$\xi(g^i) \leq \frac{1}{\phi(|g^i|)}, \qquad \text{for } i = 1, \ldots, p^n - 1,$$

where ϕ is Euler's function. ξ is a *p-adic* o.b.g.v. if

$$\xi(g^{pi}) \geq p(\xi(g^i)), \qquad \text{for } i = 0, \ldots, p^n - 1.$$

A p-adic o.b.g.v. on C_{p^2} determines, up to a unit, elements $x_{\xi(g^i)}$ in R of value $\xi(g^i)$. We use these elements to form the R-algebra

$$A(\xi) = R\left[\frac{g-1}{x_{\xi(g)}}, \frac{g^2-1}{x_{\xi(g^2)}}, \ldots, \frac{g^{p^2-1}-1}{x_{\xi(g^{p^2-1})}}\right],$$

which is an R-Hopf algebra order in KC_{p^2}. In fact, one sees that

$$A(\xi) = R\left[\frac{g^p - 1}{x_{\xi(g^p)}}, \frac{g-1}{x_{\xi(g)}}\right] = R\left[\frac{g^p - 1}{x_s}, \frac{g-1}{x_r}\right],$$

setting $\xi(g^p) = s$ and $\xi(g) = r$ (confer [U, Sect. 1.10]). We conclude that an R-Hopf order which is given by a p-adic o.b.g.v. on C_{p^2} is determined by two rationals s and r in the range of ν with $0 \le s \le 1/(p-1)$, $0 \le r \le 1/p(p-1)$, and $pr \le s$. Any such R-Hopf order H will be called a *Larson order in* KC_{p^2} and will be denoted $H(s, r)$.

As a projective module over a local ring, the Larson order $H(s, r)$ is free over R of rank p^2. It's not hard to show that an R-basis for $H(s, r)$ can be written $\{h^a k^b\}_{a,b=0,\ldots,p-1}$ where $h = (g^p - 1)/x_s$ and $k = (g-1)/x_r$ (cf. [U, Chap. 4]). Moreover, the element $\Lambda = p^2 e_0/(x_s x_r)^{p-1}$ is a generating integral for $L_{H(s,r)}$ and the element $\Lambda^* = p^2 e_0/(x_{s'} x_{r'})^{p-1}$ is a generating integral for $L_{H(s,r)^*}$ (for details, see [U, Chap. 4]). Using these facts, the following theorem due to Larson [L4, Corollary 1.2] allows us to compute an R-basis for the free R-module $H(s, r)^*$.

THEOREM 1.1.0 (Larson). *Let R be a Dedekind domain, and let H be a Hopf algebra over R. Then $L_{H^*} = R\Lambda^*$ for some integral Λ^* if and only if the map $H \to H^*$ defined by*

$$x \mapsto x \cdot \Lambda^* = \sum_{(\Lambda^*)} \langle \Lambda^*_{(1)}, \sigma_H(x) \rangle \Lambda^*_{(2)}$$

is an isomorphism of R-modules. Here $\langle\ ,\ \rangle$ denotes the duality map $H^* \times H \to R$, and $\Sigma_{(\Lambda^*)} \Lambda^*_{(1)} \otimes \Lambda^*_{(2)}$ is Sweedler notation for the image of Λ^* under Δ_{H^*}.

Therefore, an R-module basis for $H(s, r)^*$ can be written

$$\left\{ \frac{p^2\left(e_{ap} - \binom{a}{1} e_{(a-1)p} + \cdots + (-1)^a e_0\right)\left(e_b - \binom{b}{1} e_{b-1} + \cdots + (-1)^b e_0\right)}{(x_{s'} x_{r'})^{p-1} (x_s)^a (x_r)^b} \right\},$$

where $a, b = 0, 1, \ldots, p-1$.

An R-Hopf order in KC_p given by a p-adic o.b.g.v. ξ on C_p will be called a Larson order in KC_p and can be written

$$A(\xi) = R\left[\frac{g^p - 1}{x_s}\right] = H(s),$$

for some s, $0 \le s \le 1/(p-1)$. A generating integral for $L_{H(s)}$ can be written

$$\frac{p(1+g^p+\cdots+g^{p(p-1)})}{px_{(p-1)s}},$$

hence $\varepsilon_{H(s)}(L_{H(s)}) = p/x_{s(p-1)}$ (cf. [L3]).

In attempting to classify R-Hopf orders, one is naturally led to the following question: Is every R-Hopf order in KC_{p^n} a Larson order? For $n = 1$ we have the following theorem found in [U, Section 1.6].

THEOREM 1.1.1. *Let H be an R-Hopf order in KC_p. Then H is a Larson order, i.e., H is given by a p-adic o.b.g.t. on C_p.*

It follows from Theorem 1.1.1 that every R-Hopf order H in KC_p is of the form $H(s)$ for some s, $0 \le s \le 1/(p-1)$. To calculate s, we employ the Tate/Oort classification of R-Hopf orders in KC_p to write

$$H \cong R[x]/\langle x^p - bx\rangle,$$

where $u^{p-1}b = \omega_p$ is a factorization in R of a certain quantity ω_p (cf. [TO]). Then $s = v(u)$ (cf. [U, Section 1.6]).

Since $\zeta^p \in K$, the dual order $H(s)^*$ is an R-Hopf order in KC_p, and hence by Theorem 1.1.1, we have $H(s)^* = H(t)$, for some t, $0 \le t \le 1/(p-1)$. In fact we find that $H(s)^* = H(s')$, where $s' = 1/(p-1) - s$ (cf. [U] or [G]).

For $n > 1$, however, the above theorem is not true: for example, the R-Hopf order $RC_{p^2}^*$ in KC_{p^2} is not a Larson order, cf. [L3].

Every R-Hopf order in KC_{p^2} does contain a largest Larson order which we compute as follows. Let H be an R-Hopf order in KC_{p^2}, and let I_g and I_{g^p} be the fractional ideals

$$I_g = \{x \in K | x(g-1) \in H\} \quad \text{and} \quad I_{g^p} = \{x \in K | x(g^p-1) \in H\}.$$

Then the values $v(I_g^{-1}) = r$ and $v(I_{g^p}^{-1}) = s$ are so that $H(s,r)$ is the maximal Larson order contained in H. We denote the largest Larson order contained in a given R-Hopf order H by $L(H)$ (cf. [L3]).

1.2. *Greither Orders*

Greither [G] has obtained a class of R-Hopf orders in KC_{p^2} which are of the form

$$R\left[\frac{g^p-1}{x_s}, \frac{g-a_r}{x_r}\right],$$

where s and r are values from a p-adic o.b.g.v. on C_{p^2}, i.e., $0 \le s \le 1/(p-1)$, $0 \le r \le 1/(p(p-1))$, and $pr \le s$, and a_v is an element in the Larson order $H(s)$ of the form $a_v = e'_0 + ve'_1 + \cdots + v^{p-1}e'_{p-1}$, where $e'_i = (1/p)\sum_{j=0}^{p-1}\zeta^{-pij}g^{pj}$ are the idempotents of the R-algebra RC_p^*. The parameter v is a unit in

$$U_{s'e+re/p} \cap U_{s'e/p+re}$$

where $U_n = \{x \in R | x = 1 + Rp^{n/e}\}$, for any positive integer n, and e is the ramification index of p in R (cf [G, U]). An R-Hopf algebra order in KC_{p^2} of this form will be called a *Greither order* and will be denoted

$$H_v(s,r) = R\left[\frac{g^p - 1}{x_s}, \frac{g - a_v}{x_r}\right].$$

If $v = 1$, then the Greither order $H_1(s,r) = H(s,r)$, hence every Larson order is a Greither order. Suppose $H_v(s,r)$ and $H_w(s,r)$ are two Greither orders so that $v/w \in U_{s'e+re}$, then $H_v(s,r) \cong H_w(s,r)$. It follows that if $H_v(s,r)$ is a Greither order with $v \in U_{s'e+re}$, then $H_v(s,r) = H(s,r)$; cf. [G, Corollary 3.6b].

1.3. *Short Exact Sequences*

Now that we have some examples of R-Hopf algebra orders, we proceed to involve them in short exact sequences, which we now define. Suppose i: $A \to B$ is an injection of R-Hopf algebra orders, and let A^+ denote the augmentation ideal of A. If there exists a surjection of R-Hopf algebra orders P: $B \to B/i(A^+)B$, then P is said to be the *cokernel* of i. If P: $B \to C$ is any surjection of R-Hopf orders, then the subset

$$\{h \in B | (I_B \otimes P)\Delta_B(h) = h \otimes 1\}$$

is a sub R-Hopf order of B, and the injection of this sub R-Hopf order into B is defined to be the *kernel* of P. A *short exact sequence* (s.e.s.) of R-Hopf algebra orders is a sequence $A \xrightarrow{i} B \xrightarrow{P} C$, where P is the cokernel of i and i is the kernel of P. Schneider [Sc, Lemma 1.1] has shown that any R-Hopf order in KC_{p^2} will give rise to a short exact sequence.

THEOREM 1.3.0 (Schneider). *Let R be a Dedekind domain with quotient field K, and let H be a Hopf order in KC_{p^2}. Then the s.e.s. of Hopf algebras over K*

$$KC_p \xrightarrow{i} KC_{p^2} \xrightarrow{P} KC_p,$$

where P: $g^p \to 1$, *induces an s.e.s. of R-Hopf orders over* R:

$$i^{-1}(H) \xrightarrow{i} H \xrightarrow{P} P(H).$$

Note that $i^{-1}(H) = H \cap KC_p$ and $P(H)$ are R-Hopf orders in KC_p, and hence, by Theorem 1.1.1, must be Larson orders in KC_p. That is, there exists $s, r, 0 \le s,\ r \le 1/(p-1)$, so that $i^{-1}(H) = H(s)$, and $P(H) = H(r)$. The values s, r are related by the following theorem.

THEOREM 1.3.1. *Let* H *be an* R*-Hopf order in* KC_{p^2} *inducing, by Theorem* 1.3.0, *the s.e.s.* $H(s) \to H \to H(r)$. *Then* $s \ge r$.

Proof. Let $[p]$: $H \to H$ be the map defined by formal multiplication by p, that is,

$$[p](h) = \mu_H(\mu_H \otimes 1)\dots(\mu_H \otimes 1^{\otimes(p-2)})(1^{\otimes(p-2)} \otimes \Delta_H)\dots(1 \otimes \Delta_H)\Delta_H(h),$$

where μ_H: $H \otimes H \to H$ is multiplication in H. One notes that $[p]$ is a non-trivial R-Hopf algebra homomorphism, which over K yields the map $[p]$: $KC_{p^2} \to KC_{p^2}$, given by $g \mapsto g^p$, with $\mathrm{Im}([p]) = KC_p$. It follows that $[p](H) \subseteq KC_p$, and thus $[p](H) \subseteq KC_p \cap H = H(s)$. In addition, we observe that $H(s)^+H = \ker([p])$, and hence there is a Hopf algebra isomorphism $[p](H) \cong H(r)$, implying a Hopf algebra inclusion $H(r) \to H(s)$. Therefore, $r \le s$.

If H is the Greither order $H_t(s, r)$, then from Theorem 1.3.0 we obtain the s.e.s.

$$\begin{array}{ccccc} i^{-1}(H_t(s,r)) & \xrightarrow{i} & H_t(s,r) & \xrightarrow{P} & P(H_t(s,r)) \\ \| & & \| & & // \\ H(s) & \xrightarrow{i} & H_t(s,r) & \xrightarrow{P} & H(r), \end{array}$$

where $H(s)$ and $H(r)$ are Larson orders in KC_p; cf [G].

The following theorem, found in [G] as Corollary 3.6b, illustrates how Theorem 1.3.0 can be used to determine when an R-Hopf order in KC_{p^2} is a Greither order.

THEOREM 1.3.2 (Greither). *Let* H *be any* R*-Hopf order in* KC_{p^2}, *inducing the s.e.s.* $H(s) \to H \to H(r)$. *If* $pr \le s$, *then* $H = H_t(s, r)$ *for some* $v \in U_{s'e+re/p} \cap U_{s'e/p+re}$; *that is,* H *is a Greither order.*

Theorem 1.3.2 is a key theorem which will be used in the classification scheme of Part 2 (cf. Theorems 2.4 and 2.5).

We also have the following theorem which is immediate from [Sc, Section 1].

THEOREM 1.3.3. *Let H be an R-Hopf order in KC_{p^2}. The s.e.s. $H(s) \to H \to H(r)$ induces a s.e.s. of duals*:

$$H(r') \to H^* \to H(s').$$

Once we have an R-Hopf order H in KC_{p^2} involved in an s.e.s., we can use the following theorem, due to Larson [L3], to compute the ideal $\varepsilon_H(L_H)$.

THEOREM 1.3.4 (Larson). *Suppose H is an R-Hopf order in KC_{p^2}, inducing by Theorem* 1.3.0 *the s.e.s. $H(s) \to H \to H(r)$. Then*

$$\varepsilon_H(L_H) = \varepsilon_{H(s)}(L_{H(s)})\varepsilon_{H(r)}(L_{H(r)}) = \left(\frac{p}{(x_s)^{p-1}}\right)\left(\frac{p}{(x_r)^{p-1}}\right) = \frac{p^2}{(x_s x_r)^{p-1}}.$$

1.4. *The Largest Larson Order Contained in a Greither Order*

Recall that in Section 1.1 we defined $L(H)$, the largest Larson order contained in an arbitrary R-Hopf order H in KC_{p^2}. In this section we compute $L(H_t(s,r))$, the largest Larson order contained in the Greither order $H_t(s,r)$. We have the following theorem.

THEOREM 1.4.0. *Let $H_t(s,r)$ be a Greither order corresponding to some $v \in U_{s'e+re/p} \cap U_{s'e/p+re'}$. Then $L(H_1(s,r)) = H(s,r)$ and $L(H_t(s,r)) = H(s,\bar{r})$, where $\bar{r} = s + \nu(1-v) - 1/(p-1)$.*

Proof. It is immediate that $L(H_1(s,r)) = H(s,r)$. For $v \not\equiv 1 \bmod U_{s'e+re'}$, the largest Larson order $L(H)$ in $H_t(s,r)$ is, by definition, the Larson order $H(s,\bar{r})$, with $\bar{r}$ the maximum of all t with $(g-1)/x_t \in H_t(s,r)$. Since $(g-1)/x_t \mapsto (g^p-1)/x_t$ under the Hopf epimorphism $H \to H(r)$, we see that each $t \le r$. Hence,

$$\frac{g-1}{x_t} \in H_t(s,r) \Leftrightarrow \frac{g-1}{x_t} - \frac{g-a_v}{x_t} \in H_t(s,r)$$

$$\Leftrightarrow \frac{1-a_v}{x_t} \in H_t(s,r) \Leftrightarrow \frac{1-a_v}{x_t} \in H(s).$$

Now by [G, Lemma 3.2b], the last condition is equivalent to $1-v$ being divisible by $x_t x_{s'}$. Thus we seek the maximum t so that $\nu(1-v) \ge t + s'$. It follows that $\bar{r} = s + \nu(1-v) - 1/(p-1)$.

2

Now that we have reviewed the preliminary results on R-Hopf orders in KC_p and KC_{p^2}, we now state and prove the theorems which lead to the

classification of R-Hopf orders in KC_{p^2}. We begin by calculating the dual of an arbitrary Larson order $H(s, r)$ in KC_{p^2}.

THEOREM 2.0. *Let $H(s, r)$ be a Larson order in KC_{p^2}. Then $H(s, r)^* = A_\zeta(r', s')$, where $A_\zeta(r', s')$ is defined to be the $R[(g^p - 1)/x_{r'}]$-span of the elements $1, k, \ldots, k^{p-1}$, with $k = (g - a_\zeta)/x_{s'}$ and $a_\zeta = e'_0 + \zeta e'_1 + \cdots + \zeta^{p-1} e'_{p-1}$.*

Proof. We will establish this result by first showing that $A_\zeta(r', s') \subseteq H(s, r)^*$, and then showing that the discriminant of $A_\zeta(r', s')$ is equal to that of $H(s, r)^*$. This will imply that $H(s, r)^* = A_\zeta(r', s')$.

Part 1: $A_\zeta(r', s') \subseteq H(s, r)^*$. First note that the Larson order $H(s, r)$ can be viewed as the $R[(\gamma^p - 1)/x_r]$-span of the elements $1, \kappa, \kappa^2, \ldots, \kappa^{p-1}$, where $\kappa = (\gamma - 1)/x_r$, with $\langle \gamma \rangle \cong C_{p^2}$. Since $H(s, r)^*$ is an algebra, we can establish $A_\zeta(r', s') \subseteq H(s, r)^*$ by showing that $(g^p - 1)/x_{r'} \in H(s, r)^*$ and $k \in H(s, r)^*$. Now $(g^p - 1)/x_{r'} \in H(s, r)^*$ because $H(r')$ injects into $H(s, r)^*$ via the s.e.s. $H(r') \to H(s, r)^* \to H(s')$.

To show that $k \in H(s, r)^*$, it suffices to show that, for any $y \in H(s)$, the pairing $\langle y\kappa^i, k \rangle \in R$ for $i = 0, \ldots, p - 1$, where the value of $\langle y\kappa^i, k \rangle$ is induced from the relations $\langle \gamma, g \rangle = \langle \gamma^i, a_\zeta \rangle = \zeta^i$ and $\langle \gamma^{pi}, a_\zeta \rangle = 1$. The pairing $\langle y\kappa^i, k \rangle$ is, in fact, the evaluation of the functional k at $y\kappa^i$. Hence,

$$\begin{aligned}
\langle y\kappa^i, k \rangle &= k(y\kappa^i) \\
&= \mu_{KC_{p^2}}\big(\Delta_{KC_{p^2}}(k)(y \otimes \kappa^i)\big) \\
&= \mu_{KC_{p^2}}\left(g \otimes k + k \otimes a_\zeta + \frac{a_\zeta \otimes a_\zeta - \Delta_{KC_{p^2}}(a_\zeta)}{x_{s'}}\right)(y \otimes \kappa^i) \\
&\qquad\qquad \text{(cf. [G, p. 66])} \\
&= \mu_{KC_{p^2}}\big(\langle y, g \rangle \otimes \langle \kappa^i, k \rangle + \langle y, k \rangle \otimes \langle \kappa^i, a_\zeta \rangle + f(y \otimes \kappa^i)\big) \\
&= \langle y, g \rangle \langle \kappa^i, k \rangle + \langle y, k \rangle \langle \kappa^i, a_\zeta \rangle + \mu_{KC_{p^2}}\big(f(y \otimes \kappa^i)\big),
\end{aligned}$$

where $f = (a_\zeta \otimes a_\zeta - \Delta_{KC_{p^2}}(a_\zeta))/x_{s'}$. We claim that each of the above

terms is in R. To this end, observe that

$$\left\langle \left(\frac{\gamma^p - 1}{x_s}\right)^i, \frac{g - a_\zeta}{x_{s'}} \right\rangle = \left\langle \frac{(\gamma^p - 1)^i}{x_{is+s'}}, g \right\rangle - \left\langle \frac{(\gamma^p - 1)^i}{x_{is+s'}}, a_\zeta \right\rangle$$

$$= \frac{(\zeta^p - 1)^i}{x_{is+s'}} - \frac{1}{x_{is+s'}} \sum_{j=0}^{i} (-1)^j \binom{i}{j}$$

$$= \frac{(\zeta^p - 1)^i}{x_{is+s'}} \in R, \qquad \text{since } s + s' = \frac{1}{p-1}.$$

Thus $\langle y, k \rangle \in R$. Another direct calculation yields $\langle \kappa^i, k \rangle = 0$. Additionally, by [G, Lemma 3.2b], $a_\zeta \in H(r') \subseteq H(s, r)^*$, and hence $\langle \kappa^i, a_\zeta \rangle \in R$. As a consequence of Greither's lemma, we also have that $f \in H(r') \otimes H(r')$, which yields $\mu_{KC_{p^2}}(f(y \otimes \kappa^i)) \in R$ (cf. [G, p. 66]). It follows that $k \in H(s, r)^*$, and thus, $A_\zeta(r', s') \subseteq H(s, r)^*$.

The conditions $a_\zeta \in H(r')$ and $f \in H(r') \otimes H(r')$ also imply that

$$\Delta_{KC_{p^2}}(k) = g \otimes k + k \otimes a_\zeta + \frac{a_\zeta \otimes a_\zeta - \Delta_{KC_{p^2}}(a_\zeta)}{x_{s'}} \in A_\zeta(r', s') \otimes A_\zeta(r', s').$$

Moreover, it is easy to show that

$$\Delta_{KC_{p^2}}\left(\frac{g^p - 1}{x_{r'}}\right) \in H(r') \otimes H(r') \subseteq A_\zeta(r', s') \otimes A_\zeta(r', s'),$$

thus, the *algebra* $A_\zeta(r', s')$ (with multiplication induced from KC_{p^2}) is an R-Hopf algebra.

Part 2: $A_\zeta(r', s') = H(s, r)^*$. Our goal is to show that

$$\operatorname{disc}\big(A_\zeta(r', s')/R\big) = \operatorname{disc}\big(H(s, r)^*/R\big),$$

and therefore $A_\zeta(r', s') = H(s, r)^*$. We first need some preliminary information about discriminants. Suppose that $N \subseteq M$ are free R-modules of the same rank m. Let $\{b_0, \ldots, b_{m-1}\}$ be a basis for M and let $\{\sum_{i=0}^{m-1} a_{ij} b_i\}_{j=0,\ldots,m-1}$ be a basis for N. Let $J(M, N)$ be the ideal generated by $\det(A)$ where A is the matrix (a_{ij}). Under these conditions we have

$$\operatorname{disc}(N/R) = J(M, N)^2 \cdot \operatorname{disc}(M/R). \tag{1}$$

(cf. [G, Lemma 1.1a]). Note that if P is a free R-module of rank m with

$P \subseteq N \subseteq M$, then

$$J(M, P) = J(N, P) \cdot J(M, N). \tag{2}$$

We are now in a position to calculate $\operatorname{disc}(A_\zeta(r', s')/R)$. We begin by writing the inclusion $RC_{p^2} \subseteq A'_\zeta \subseteq A_\zeta(r', s')$ where A'_ζ is that free R-module with basis

$$\left\{ \left(\frac{g^p - 1}{x_{r'}} \right)^i, (g - a_\zeta)^j \right\}.$$

We then use the transitivity formula (2) to calculate $J(A_\zeta(r', s'), RC_{p^2})$. Note that $J(A_\zeta(r', s'), A'_\zeta)$, by definition, is the ideal generated by

$$(x_{s'})^{0+p+2p+\cdots+(p-1)p}.$$

In addition, we see that $A'_\zeta = H_\zeta(r', 0)$ is the Larson order $H(r', 0)$ because $\nu(1 - \zeta) = 1/(p(p-1)) \geq r$, cf. Section 1.2. Since A'_ζ is a Larson order, an R-basis for A'_ζ can be written as

$$\left\{ \left(\frac{g^p - 1}{x_{r'}} \right)^i, \left(\frac{g - 1}{x_0} \right)^j \right\}.$$

Thus $J(A'_\zeta, RC_{p^2})$ is generated by

$$(x_{r'})^{0+p+2p+\cdots+(p-1)p}.$$

It follows from the transitivity formula (2) that

$$J\left(A_\zeta(r', s'), RC_{p^2}\right) = (x_{s'}x_{r'})^{p+2p+\cdots+(p-1)p}.$$

Noting that $RC_{p^2} \subseteq A_\zeta(r', s')$, and that $\operatorname{disc}(RC_{p^2}/R) = (p^2)^{p^2}$, and employing formula (1), we obtain

$$\begin{aligned}
\operatorname{disc}\left(A_\zeta(r', s')/R\right) &= \frac{(p^2)^{p^2}}{\left((x_{s'}x_{r'})^{p+2p+\cdots+(p-1)p}\right)^2} \\
&= \frac{(p^2)^{p^2}}{\left((x_{s'}x_{r'})^{p(1+2+\cdots+p-1)}\right)^2} \\
&= \frac{(p^2)^{p^2}}{(x_{s'}x_{r'})^{p(p(p-1))}} \\
&= \left(\frac{(p^2)}{(x_{s'}x_{r'})^{p-1}} \right)^{p^2}.
\end{aligned}$$

We now compute $\operatorname{disc}(H(s,r)^*/R)$ and find that

$$\begin{aligned}
\operatorname{disc}(H(s,r)^*/R) &= \left(\varepsilon_{H(s,r)^*}(L_{H(s,r)^*})\right)^{p^2} \qquad \text{(cf. [G, Lemma 1.3a])} \\
&= \left(\varepsilon_{H(s')}(L_{H(s')})\varepsilon_{H(r')}(L_{H(r')})\right)^{p^2} \qquad \text{(by Theorem 1.3.4)} \\
&= \left(\left(\frac{p}{x_{(p-1)s'}}\right)\left(\frac{p}{x_{(p-1)r'}}\right)\right)^{p^2} \\
&= \left(\frac{p^2}{(x_{s'}x_{r'})^{p-1}}\right)^{p^2} \qquad \text{(by Section 1.1).}
\end{aligned}$$

Thus $\operatorname{disc}(H(s,r)^*/R) = \operatorname{disc}(A_\zeta(r',s')/R)$ and hence $H(s,r)^* = A_\zeta(r',s')$.

COROLLARY 2.1. *Suppose $H(s,r)$ is a Larson order in KC_{p^2}, and suppose $ps' \le r'$. Then $H(s,r)^* = A_\zeta(r',s')$ is the Greither order $H_\zeta(r',s')$.*

COROLLARY 2.2. *Suppose $H(s,r)$ is a Larson order in KC_{p^2}, and suppose $ps' \le r'$ and $s \ge 1/p + r$. Then $H(s,r)^* = A_\zeta(r',s') = H_\zeta(r',s') = H(r',s')$; i.e., the dual of the Larson order $H(s,r)$ is the Larson order $H(r',s')$.*

Proof. The condition $ps' \le r'$ implies that $H(s,r)^*$ is the Greither order $H_\zeta(r',s')$. Note that $s \ge 1/p + r$ if and only if $v = \zeta \in U_{re+s'e}$, so that, by Section 1.2, we have $H_\zeta(r',s') = H(r',s')$.

Remark 2.3. Compare Theorem 2.0 and Corollary 2.1 with Remark 3.12 in [G].

With Theorem 1.3.2 in mind, which tells us when an arbitrary R-Hopf order is a Greither order, we now prove Theorems 2.4 and 2.5.

THEOREM 2.4. *Suppose H is an R-Hopf order in KC_{p^2}, inducing the s.e.s. $H(s) \to H \to H(r)$ and the dual s.e.s. $H(r') \to H^* \to H(s')$. Suppose $s \ge 1/p$. Then if $r \ge s'$, we have $ps' \le r'$, and if $s' \ge r$, then $pr \le s$.*

Proof. Since $H(s)$ injects into H, we have that the Larson order $H(s,0) \subseteq H$. Hence $H^* \subseteq H(s,0)^*$. But note that $s \ge 1/p + 0$, and therefore by Corollary 2.2, we conclude that $H^* \subseteq H(s,0)^* = H(1/(p-1), s')$. Recall that $\{h^a k^b\}$ for $a, b = 0, 1, \ldots, p-1$ with $h = (g^p - 1)/x_{1/(p-1)}$ and $k = (g-1)/x_{s'}$ is an R-basis for $H(1/(p-1), s')$ (cf. Section 1.1). Hence a basis for H^* is given by the matrix product

$$(k, \ldots, k^{p-1}, hk, hk^2, \ldots, h^{p-1}k^{p-1}, 1, h, \ldots, h^{p-1}) \cdot M,$$

where M is some $p^2 \times p^2$ matrix with entries in R. Since R is a discrete valuation ring, we may perform elementary column operations on the matrix M so that it has the (equivalent) upper-triangular form

$$M' = \begin{pmatrix} r_{11} & r_{12} & \cdots & \cdots & r_{1p^2} \\ 0 & r_{22} & \cdots & \cdots & r_{2p^2} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & r_{p^2p^2} \end{pmatrix}$$

with $r_{ij} \in R$, and with either $r_{ij} = 0$ or $\nu(r_{ij}) > \nu(r_{i(j+1)})$, for all i, j. Let $\{\alpha_j\}$ denote this basis for H^*, where $\alpha_j = \sum_{i=1}^{p^2} r_{ij} h^a k^b$ with a, b integers $0 \le a, b \le p-1$, dependent on i; that is, considering the ordering of the elements

$$\{k, \ldots, k^{p-1}, hk, hk^2, \ldots, h^{p-1}k^{p-1}, 1, h, \ldots, h^{p-1}\},$$

we have that $i = 1 \Leftrightarrow (a, b) = (0, 1)$, $i = 2 \Leftrightarrow (a, b) = (0, 2)$, and so on.

Let $\{\bar{\alpha}_j\}$ denote the image of this basis under the map $g^p \mapsto 1$. Because $g^p \mapsto 1$ is a module surjection, the span of $\{\bar{\alpha}_j\}$ must be $H(s')$. Thus, we can assume that $r_{1j_1} = r_{2j_2} = \cdots = r_{(p-1)j_{p-1}} = 1$ for some integers j_c, $1 \le j_c \le p^2$. In fact, we claim that each $j_c \le p^2 - p$. To see this, first note that $H^* \cong H(s') \otimes H(r')$ as right $H(r')$-modules, and hence as R-modules (confer [Sc, Sect. 1]), and the elements

$$\left\{ \left(\frac{\bar{g} - 1}{x_{s'}} \right)^b \otimes_R \left(\frac{g^p - 1}{x_{r'}} \right)^a \right\}$$

form an R-basis for H^*. (Here $\bar{g}$ denotes the image of g under the map $g^p \mapsto 1$.) Identifying the elements $\{1 \otimes_R ((g^p - 1)/x_{r'})^a\}$ with the basis $\{x_{ar}h^a\}$ of $H(r')$, we can write the R-direct sum $H^* \cong S \oplus H(r')$, where S is some R-module. It follows that any R-linear combination of the basis $\{k, \ldots, k^{p-1}, hk, hk^2, \ldots, h^{p-1}k^{p-1}, 1, h, \ldots, h^{p-1}\}$ which is in H^* is, in fact, an R-linear combination of the elements

$$\{k, \ldots, k^{p-1}, hk, hk^2, \ldots, h^{p-1}k^{p-1}, 1, x_r h, \ldots, x_{(p-1)r}h^{p-1}\}. \quad (3)$$

Specifically, the basis $\{\alpha_j\}$ for H^* consists of R-linear combinations of (3). Now to generate $H(r') \subseteq H^*$ using $\{\alpha_j\}$, we need at least the last p columns of M', but because $\nu(r_{ij}) > \nu(r_{i(j+1)})$ for all i, j, when $r_{ij} \neq 0$, we need *only* these columns. Hence the last p columns of M' form a basis for $H(r')$. From this we conclude that each $j_c \le p^2 - p$.

Hence with $j = j_1$, we have

$$\rho^* = \sum_{i=1}^{p^2} r_{ij} h^a k^b = k + \sum_{i=2}^{p^2} r_{ij} h^a k^b \in H^*,$$

where $r_{ij} = 0$ for $i > j$ (since M' is upper-triangular). The reader should note that this last condition implies $r_{ij} = 0$ for those i whose corresponding pairs $(a, b) = (0,0), (1,0), \ldots, (p-1, 0)$, i.e., for those i with $i \geq p^2 - (p-1)$.

Our plan for the proof of Theorem 2.4 is to show that the pth power of ρ^* is congruent mod H^* to an element in $H(r')$ whose representation with respect to the basis $\{((g^p - 1)/x_{r'})^a\}$ contains the term $(g^p - 1)/x_{ps'}$. Then by comparing coefficients, we can conclude that $ps' \leq r'$.

By a direct calculation we find that

$$(\rho^*)^p = \left(k + \sum_{i=2}^{j} r_{ij} h^a k^b\right)^p$$

$$= (k)^p + \sum_{i=2}^{j} \left(r_{ij} h^a k^b\right)^p + \sum pu \prod_{i=1}^{j} \left(r_{ij} h^a k^b\right)^{N_i} \in H^*,$$

where the last summation is over all partitions $\Sigma N_i = p$, and u is a unit in R dependent on the partition. We claim that

$$\sum pu \prod_{i=1}^{j} \left(r_{ij} h^a k^b\right)^{N_i}$$

is in H^*. We prove this by first obtaining a lower bound on the value of the coefficients r_{ij}. Indeed, we claim that $\nu(r_{ij}) \geq ar + bs' - (p-1)s'$. To this end, note that since

$$\Lambda = \frac{p^2 e_0}{(x_s x_r)^{p-1}}$$

is a generating integral for H, we have that $\rho = \rho^* \cdot \Lambda =$

$$\sum_{i=1}^{p^2} \frac{p^2 r_{ij}}{(x_s x_r)^{p-1}} \left(\frac{e_{ap} - \binom{a}{1} e_{(a-1)p} + \cdots + (-1)^a e_0}{(x_{1/(p-1)})^a}\right)$$

$$\times \left(\frac{e_b - \binom{b}{1} e_{b-1} + \cdots + (-1)^b e_0}{(x_{s'})^b}\right) \in H.$$

Note also that $H(r',0) \subseteq H^*$ implies $H \subseteq H(r',0)^* = R[(g^p - 1)/x_{r'}, (g-1)/x_0]^*$. In addition, a generating integral for $H(r',0)^*$ is $p^2 e_0/(x_{1/(p-1)}x_r)^{p-1}$, hence a basis for $H(r',0)^*$ can be written

$$\left\{ \frac{p^2}{(x_{1/(p-1)}x_r)^{p-1}} \frac{1}{x_{ar'}} \left(e_{ap} - \binom{a}{1} e_{(a-1)p} + \cdots + (-1)^a e_0 \right) \right.$$
$$\left. \times \left(e_b - \binom{b}{1} e_{b-1} + \cdots + (-1)^b e_0 \right) \right\},$$

where a, b are integers $0 \le a,\ b \le p-1$. Since $H \subseteq H(r',0)^*$, the element ρ must be an integral linear combination of the basis for $H(r',0)^*$. Note that for each $i = 1, \ldots, p^2$,

$$\frac{p^2 r_{ij}}{(x_s x_r)^{p-1}} \left(\frac{e_{ap} - \binom{a}{1} e_{(a-1)p} + \cdots + (-1)^a e_0}{(x_{1/(p-1)})^a} \right)$$
$$\times \left(\frac{e_b - \binom{b}{1} e_{b-1} + \cdots + (-1)^b e_0}{(x_{s'})^b} \right)$$
$$= \frac{r_{ij} x_{ar'}}{(x_s)^{p-1} x_{bs'} x_{((a-p+1/(p-1))}}$$
$$\times \left(\frac{p^2}{(x_{1/(p-1)}x_r)^{p-1}} \frac{1}{x_{ar'}} \left(e_{ap} - \binom{a}{1} e_{(a-1)p} + \cdots + (-1)^a e_0 \right) \right.$$
$$\left. \times \left(e_b - \binom{b}{1} e_{b-1} + \cdots + (-1)^b e_0 \right) \right),$$

where a, b are integers $0 \le a,\ b \le p-1$. Thus, we must have

$$\nu(r_{ij}) + ar' \ge (p-1)s + bs' + \frac{a-p+1}{p-1}$$

$$\nu(r_{ij}) + \frac{a}{p-1} - ar \ge s + s' + (p-2)s + (b-1)s' + \frac{a-p+1}{p-1}$$

$$\nu(r_{ij}) \geq ar + \frac{1}{p-1} + (b-1)s' + (p-2)s + \frac{1-p}{p-1}$$

$$\nu(r_{ij}) \geq ar + (b-1)s' + (2-p)\left(\frac{1}{p-1} - s\right)$$

$$\nu(r_{ij}) \geq ar + (b-1)s' - (p-2)s'$$

$$\nu(r_{ij}) \geq ar + (b-(p-1))s' = ar + bs' - (p-1)s'.$$

Now we are in a position to show that $\Sigma pu\prod_{i=1}^{j}(r_{ij}h^ak^b)^{N_i} \in H^*$. Indeed, with $n \geq 0$, so that $(x_n(x_r)^a(x_{s'})^b)/x_{(p-1)s'} = r_{ij}$, we have

$$\begin{aligned}
&\sum pu\prod_{i=1}^{j}\left(r_{ij}h^ak^b\right)^{N_i} \\
&\quad = \sum pu\prod_{i=1}^{j}\left(r_{ij}\left(\frac{g^p-1}{x_{1/(p-1)}}\right)^a\left(\frac{g-1}{x_{s'}}\right)^b\right)^{N_i} \\
&\quad = \sum pu\prod_{i=1}^{j}\left(x_n\left(\frac{x_r(g^p-1)}{x_{1/(p-1)}}\right)^a\frac{1}{x_{(p-1)s'}}\left(\frac{x_{s'}(g-1)}{x_{s'}}\right)^b\right)^{N_i} \\
&\quad = \sum pu\prod_{i=1}^{j}\left(x_n\left(\frac{g^p-1}{x_{r'}}\right)^a\frac{1}{x_{(p-1)s'}}\left(\frac{g-1}{1}\right)^b\right)^{N_i} \\
&\quad = \sum pu\frac{1}{x_{\sum N_i(p-1)s'}}\prod_{i=1}^{p^2}\left(x_n\left(\frac{g^p-1}{x_{r'}}\right)^a\left(\frac{g-1}{1}\right)^b\right)^{N_i}.
\end{aligned}$$

Now since $\Sigma N_i = p$ and $s' \leq 1/p(p-1)$, we must have

$$pu1/x_{\sum N_i(p-1)s'} \in R.$$

Hence

$$\sum pu\frac{1}{x_{\sum N_i(p-1)s'}}\prod_{i=1}^{j}\left(x_n\left(\frac{g^p-1}{x_{r'}}\right)^a\left(\frac{g-1}{1}\right)^b\right)^{N_i} \in H^*.$$

We conclude that

$$(k)^p + \sum_{i=2}^{j}\left(r_{ij}h^ak^b\right)^p \in H^*.$$

With $k = (g-1)/x_{s'}$ and $h = (g^p - 1)/x_{1/p-1}$, we can write

$$
\begin{aligned}
&(k)^p + \sum_{i=2}^{j} \left(r_{ij} h^a k^b\right)^p \\
&\quad = \left(\frac{g-1}{x_{s'}}\right)^p + \sum_{a+b<p} (r_{ij})^p \left(\left(\frac{g^p-1}{x_{1/p-1}}\right)^p\right)^a \left(\left(\frac{g-1}{x_{s'}}\right)^p\right)^b \\
&\qquad + \sum_{a+b\geq p} (r_{ij})^p \left(\left(\frac{g^p-1}{x_{1/p-1}}\right)^p\right)^a \left(\left(\frac{g-1}{x_{s'}}\right)^p\right)^b,
\end{aligned}
$$

where the first sum in the above expression is over i, $i = 2, \ldots, j$, so that the corresponding (a, b) satisfies $a + b < p$, and the second sum is over those i, $i = 2, \ldots, j$, satisfying $a + b \geq p$.

Expanding pth powers in this expression yields

$$
\begin{aligned}
&\frac{g^p-1}{x_{ps'}} + \frac{1}{x_{ps'}} \sum_{\iota=1}^{p-1} (-1)^\iota \binom{p}{\iota} g^{p-\iota} \\
&\qquad + \sum_{a+b<p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} g^{p\iota} \left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a \\
&\qquad\quad \times \left(\frac{g^p-1}{x_{ps'}} + \frac{1}{x_{ps'}} \sum_{\iota=1}^{p-1} (-1)^\iota \binom{p}{\iota} g^{p-\iota}\right)^b \\
&\qquad + \sum_{a+b\geq p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} g^{p\iota} \left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a \\
&\qquad\quad \times \left(\frac{g^p-1}{x_{ps'}} + \frac{1}{x_{ps'}} \sum_{\iota=1}^{p-1} (-1)^\iota \binom{p}{\iota} g^{p-\iota}\right)^b \\
&\quad = \frac{g^p-1}{x_{ps'}} + \frac{1}{x_{ps'}} \sum_{\iota=1}^{p-1} (-1)^\iota \binom{p}{\iota} g^{p-\iota} \\
&\qquad + \sum_{a+b<p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} g^{p\iota} \left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a \\
&\qquad\quad \times \left(\left(\frac{g^p-1}{x_{ps'}}\right)^b + \sum_{\tau=1}^{b} (-1)^\tau \binom{b}{\tau}\right.
\end{aligned}
$$

$$\times\left(\frac{g^p-1}{x_{ps'}}\right)^{b-\tau}\left(\frac{1}{x_{ps'}}\sum_{\iota=1}^{p-1}(-1)^{\iota}\binom{p}{\iota}g^{p-\iota}\right)^{\tau}\Bigg)$$

$$+\sum_{a+b\geq p}(r_{ij})^p\left(\sum_{\iota=1}^{(p-1)/2}(-1)^{\iota}\binom{p}{\iota}g^{p\iota}\left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a$$

$$\times\left(\left(\frac{g^p-1}{x_{ps'}}\right)^b+\sum_{\tau=1}^{b}(-1)^{\tau}\binom{b}{\tau}\left(\frac{g^p-1}{x_{ps'}}\right)^{b-\tau}\right.$$

$$\left.\times\left(\frac{1}{x_{ps'}}\sum_{\iota=1}^{p-1}(-1)^{\iota}\binom{p}{\iota}g^{p-\iota}\right)^{\tau}\right)$$

$$=\frac{g^p-1}{x_{ps'}}+\sum_{a+b<p}(r_{ij})^p$$

$$\times\left(\sum_{\iota=1}^{(p-1)/2}(-1)^{\iota}\binom{p}{\iota}u_{\iota}\left(\frac{g^p-1}{x_{p/p-1}}\right)\right)^a\left(\frac{g^p-1}{x_{ps'}}\right)^b$$

$$+\sum_{a+b\geq p}(r_{ij})^p\left(\sum_{\iota=1}^{(p-1)/2}(-1)^{\iota}\binom{p}{\iota}u_{\iota}\left(\frac{g^p-1}{x_{p/p-1}}\right)\right)^a$$

$$\times\left(\frac{g^p-1}{x_{ps'}}\right)^b+A+B+C$$

with

$$A=\frac{1}{x_{ps'}}\sum_{\iota=1}^{p-1}(-1)^{\iota}\binom{p}{\iota}g^{g-\iota}$$

$$B=\sum_{a+b<p}(r_{ij})^p\left(\sum_{\iota=1}^{(p-1)/2}(-1)^{\iota}\binom{p}{\iota}g^{p\iota}\left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a$$

$$\times\left(\sum_{\tau=1}^{b}(-1)^{\tau}\binom{b}{\tau}\left(\frac{g^p-1}{x_{ps'}}\right)^{b-\tau}\left(\frac{1}{x_{ps'}}\sum_{\iota=1}^{p-1}(-1)^{\iota}\binom{p}{\iota}g^{p-\iota}\right)^{\tau}\right)$$

$$C=\sum_{a+b\geq p}(r_{ij})^p\left(\sum_{\iota=1}^{(p-1)/2}(-1)^{\iota}\binom{p}{\iota}g^{p\iota}\left(\frac{g^{p(p-2\iota)}-1}{x_{p/p-1}}\right)\right)^a$$

$$\times\left(\sum_{\tau=1}^{b}(-1)^{\tau}\binom{b}{\tau}\left(\frac{g^p-1}{x_{ps'}}\right)^{b-\tau}\left(\frac{1}{x_{ps'}}\sum_{\iota=1}^{p-1}(-1)^{\iota}\binom{p}{\iota}g^{p-\iota}\right)^{\tau}\right).$$

We claim that A, B, C are in H^*. Note that $A \in H^*$ because $s' \leq 1/p(p-1)$. To show that B is in H^*, observe that $a + b < p$ implies

$$\tau - \frac{a+b}{p-1} \geq -(a+b-\tau)r', \qquad \text{for } 1 \leq \tau \leq b,$$

which gives $B \in H^*$. Moreover, $\nu(r_{ij}) \geq ar + bs' - (p-1)s'$, $r \geq s'$, and $a + b \geq p$ imply $\nu(r_{ij}) \geq (a+b-p+1)r \geq 0$, hence

$$\begin{aligned}
&\nu(r_{ij}) + \tau - \left(\frac{a+b}{p-1}\right) \\
&\quad \geq (a+b-p+1)r + \tau - \left(\frac{a+b}{p-1}\right) \\
&\quad \geq -\left(\frac{a+b}{p-1}\right) + 1 + (a+b-p+1)r \\
&\quad \geq -(a+b-p+1)\left(\frac{1}{p-1} - r\right) = -(a+b-p+1)r',
\end{aligned}$$

from which we conclude $C \in H^*$. It follows that

$$\begin{aligned}
&\frac{g^p - 1}{x_{ps'}} + \sum_{a+b<p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} u_\iota \left(\frac{g^p - 1}{x_{p/p-1}} \right) \right)^a \left(\frac{g^p - 1}{x_{ps'}} \right)^b \\
&\quad + \sum_{a+b\geq p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} u_\iota \left(\frac{g^p - 1}{x_{p/p-1}} \right) \right)^a \left(\frac{g^p - 1}{x_{ps'}} \right)^b \in H^*.
\end{aligned}$$

We now claim that the terms

$$\sum_{a+b\geq p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} u_\iota \left(\frac{g^p - 1}{x_{p/p-1}} \right) \right)^a \left(\frac{g^p - 1}{x_{ps'}} \right)^b$$

are in H^*. For this, employ the inequality $\nu(r_{ij}) \geq (a+b-p+1)r \geq 0$,

to obtain

$$\begin{aligned}
&\nu(r_{ij}) + 1 - \left(\frac{a+b}{p-1}\right) \\
&\quad \geq (a+b-p+1)r + 1 - \left(\frac{a+b}{p-1}\right) \\
&\quad \geq -\left(\frac{a+b}{p-1}\right) + 1 + (a+b-p+1)r \\
&\quad \geq -(a+b-p+1)\left(\frac{1}{p-1} - r\right) = -(a+b-p+1)r',
\end{aligned}$$

which says

$$\sum_{a+b\geq p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} u_\iota \left(\frac{g^p-1}{x_{p/p-1}}\right)\right)^a \left(\frac{g^p-1}{x_{ps'}}\right)^b \in H^*.$$

We conclude that

$$\frac{g^p-1}{x_{ps'}} + \sum_{a+b<p} (r_{ij})^p \left(\sum_{\iota=1}^{(p-1)/2} (-1)^\iota \binom{p}{\iota} u_\iota \left(\frac{g^p-1}{x_{p/p-1}}\right)\right)^a \left(\frac{g^p-1}{x_{ps'}}\right)^b$$

is in H^*.

Now since this quantity is in $KC_p \cap H^* = H(r')$, and $\{((g^p-1)/x_{r'})^a\}$ forms an R-basis for $H(r')$, we must have that $ps' \leq r'$.

To conclude the proof of Theorem 2.4, suppose that $s \geq 1/p$, with $s' \geq r$. Then necessarily, $r' \geq 1/p$. Hence by a symmetric argument we obtain $pr \leq s$.

THEOREM 2.5. *Let H be an R-Hopf algebra order in KC_{p^2}. Let $H(s) \to H \to H(r)$ be the corresponding s.e.s. dualizing as $H(r') \to H^* \to H(s')$. Then if $s < 1/p$, we have $r' \geq 1/p$ and $s' \geq r$.*

Proof. We have the inclusion $H(s,0) \subseteq H$, implying the inclusion $H^* \subseteq H(s,0)^* = A_\zeta(1/(p-1), s')$, by Theorem 2.0. From the construction of $A_\zeta(1/(p-1), s')$, it is clear that an R-basis for $A_\zeta(1/(p-1), s')$ consists of $\{h^a k^b\}_{a,b=0,\ldots,p-1}$, where $h = (g^p-1)/x_{1/(p-1)}$ and $k = (g-a_\zeta)/x_{s'}$ (cf. proof of Theorem 2.0). Moreover, as in the proof of Theorem 2.4, we may view H^* as an R-direct sum $S \oplus H(r') \subseteq A_\zeta(1/(p-1), s')$, for some R-module S, and hence write an R-basis B for H^*

which consists of R-linear combinations of the elements

$$\{k, \ldots, k^{p-1}, hk, hk^2, \ldots, h^{p-1}k^{p-1}, 1, x_r h, \ldots, x_{(p-1)r}h^{p-1}\}. \quad (3)$$

Now observe that $s < 1/p$ implies $s' > 1/p(p-1)$, and thus $ps' > 1/(p-1) \geq r'$, which says that H^* is not a Larson order. H^* does contain the maximal Larson order $L(H^*)$, however, and thus contains the element $(g-1)/x_t$, for some $t \geq 0$. The element $(g-1)/x_t \in H^*$ can be written as a linear combination of the basis B, and when we combine like terms in this linear combination we obtain, for various $r_i \in R$,

$$\frac{g-1}{x_t} = \sum_{i=1}^{p^2} r_i h^a k^b = \sum_{i=1}^{p^2} r_i \left(\frac{g^p - 1}{x_{1/(p-1)}}\right)^a \left(\frac{g - a_\zeta}{x_{s'}}\right)^b$$

$$= \sum_{i=1}^{p^2} r_i \left(\frac{g^p - 1}{x_{1/(p-1)}}\right)^a \left(\frac{g-1}{x_{s'}} + \frac{1 - a_\zeta}{x_{s'}}\right)^b$$

with a, b dependent on i; i.e., considering the ordering of the elements in (3), we have that $i = 1 \Leftrightarrow (a, b) = (0, 1)$, $i = 2 \Leftrightarrow (a, b) = (0, 2)$, and so on. Moreover, the reader should note that $\nu(r_i) \geq ar$ for those i with $i \geq p^2 - (p-1)$.

Note that if $(g-1)/x_t$ is to be obtained as such a linear combination, then $r_i = 0$, for those i whose corresponding pairs (a, b) are other than $(0,0), (1,0), \ldots, (p-1, 0)$, and $(0, 1)$. Hence

$$\frac{g-1}{x_t} = r_1\left(\frac{g-1}{x_{s'}} + \frac{1-a_\zeta}{x_{s'}}\right) + \sum_{i=p^2-p+1}^{p^2} r_i \left(\frac{g^p - 1}{x_{1/(p-1)}}\right)^a,$$

where $\nu(r_i) \geq ar$, for $i = p^2 - (p-1), \ldots, p^2$. It follows that r_1 is such that $r_1(1 - a_\zeta)/x_{s'} \in H(r') = R[(g^p - 1)/x_r]$. Additionally, we must have $\nu(r_1) \leq s'$, for if $\nu(r_1) > s'$, then

$$\frac{g-1}{x_t} = r_1\left(\frac{g-1}{x_{s'}} + \frac{1-a_\zeta}{x_{s'}}\right) + \sum_{i=p^2-p+1}^{p^2} r_i \left(\frac{g^p - 1}{x_{1/(p-1)}}\right)^a$$

with $t \geq 0$ is not possible. Hence $\nu(r_1) \leq s'$, and therefore $1 - a_\zeta \in H(r')$, which by [G, Lemma 3.2b] yields $r' \geq 1/p$.

We conclude the proof by noting that $s < 1/p$ implies $s' > 1/p(p-1)$, and $r' \geq 1/p$ implies $r \leq 1/p(p-1)$; thus $s' \geq r$.

We are now in a position to prove the main theorem.

THEOREM 2.6. *Let H be an R-Hopf order in KC_{p^2}. Then H is either a Greither order, or its dual H^* is a Greither order.*

Proof. We begin by noting that the R-Hopf order H will induce a s.e.s. $H(s) \to H \to H(r)$ which dualizes as $H(r') \to H^* \to H(s')$.

Case 1: $s \geq 1/p$. Suppose also that $r \geq s'$. Then by Theorem 2.4 we conclude that $ps' \leq r'$, and by Theorem 1.3.2 we have that H^* is a Greither order. If $s \geq 1/p$ with $s' \geq r$, then by Theorem 2.4 we have $pr \leq s$, and thus by Theorem 1.3.2 H is a Greither order.

Case 2: $s < 1/p$. If $s < 1/p$, then we must have $r' \geq 1/p$ and $s' \geq r$, by Theorem 2.5. Hence, by Theorems 2.4 and 1.3.2, we conclude that H is a Greither order.

Using Theorem 2.6 we see that if H is an arbitrary R-Hopf order in KC_{p^2}, and $H(s) \to H \to H(r)$ is the induced s.e.s., then either $pr \leq s$, with $s \leq 1/(p-1)$ and $r \leq 1/(p(p-1))$, or $ps' \leq r'$, with $r' \leq 1/(p-1)$ and $s' \leq 1/p(p-1)$. Hence the pair (r, s) is a point in the shaded region of Fig. 2.7.

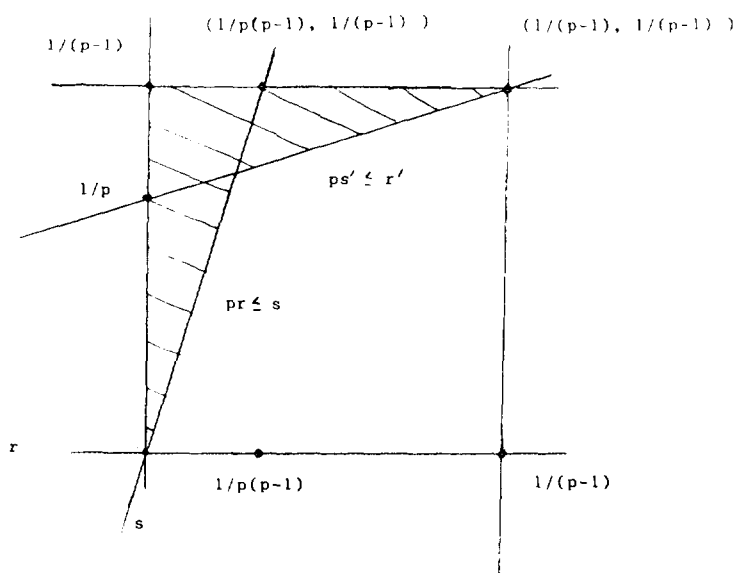

FIGURE 2.7.

REFERENCES

[A] M. F. ATIYAH, AND I. G. MACDONALD, "Introduction to Commutative Algebra," Addison-Wesley, Reading, MA, 1969.

[B] K. BROWN, "Cohomology of Groups," Springer-Verlag, New York, 1982.

[C] L. N. CHILDS, Taming wild extensions with Hopf algebras, *Trans. Amer. Math. Soc.* **304**, No. 1 (1987).

[CF] J. W. S. CASSELS AND A. FRÖHLICH (Eds.), "Algebraic Number Theory," Academic Press, New York, 1967.

[DG] M. DEMAZURE AND P. GABRIEL, "Groupes Algebrique," Vol. 1, North-Holland, Amsterdam, 1970.

[G] C. GREITHER, Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring, *Math. Z.* **210** (1992), 37–67.

[HS] P. J. HILTON AND U. STAMMBACH, "A Course in Homological Algebra," Springer-Verlag, New York, 1970.

[HK] K. HOFFMAN AND R. KUNZE, "Linear Algebra," 2nd ed., Prentice–Hall, , Englewood Cliffs, NJ, 1961.

[J] J. C. JANTZEN, "Representations of Algebraic Groups," Academic Press, New York, 1987.

[L] S. LANG, "Algebra," 2nd ed., Addison-Wesley, New York, 1984.

[L1] R. G. LARSON, Characters of Hopf algebras, *J. Algebra* **17**, (1971), 352–368.

[L2] R. G. LARSON, Hopf algebras via symbolic algebra, *in* "Computers in Algebra," (Tangora, Ed.), pp. 91–97.

[L3] R. G. LARSON, Hopf algebra orders determined by group valuations, *J. Algebra* **38** (1976), 414–452.

[L4] R. G. LARSON, Orders in Hopf algebras, *J. Algebra* **22** (1972), 201–210.

[L5] R. G. LARSON, Group rings over Dedekind domains, *J. Algebra* **5** (1967), 358–361.

[LS] R. G. LARSON AND M. SWEEDLER, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* (1967), 75–93.

[M] S. MACLANE, "Homology," Academic Press, New York, 1963.

[Mi] J. S. MILNE, "Etale Cohomology," Princeton Univ. Press, Princeton, NJ, 1980.

[N] K. NEWMAN, A correspondence between bi-ideals and sub-Hopf algebras in cocommutative Hopf algebras, *J. Algebra* **36** (1975), 1–15.

[S] P. SAMUEL, "Algebraic Theory of Numbers," Houghton Mifflin, Boston, 1970.

[Sc] H-J. SCHNEIDER, Cartan matrix of liftable finite group schemes, *Comm. Algebra* **5**, No. 8 (1977), 795–819.

[Sh] I. R. SHAFAREVICH, "Basic Algebraic Geometry," Springer-Verlag, New York, 1974.

[Sp] E. H. SPANIER, "Algebraic Topology," Springer-Verlag, New York, 1966.

[Sw] M. E. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.

[T] S. TAKAHASHI, A characterization of group rings as a special class of Hopf algebras, *Canad. Bull. Math.* **8**, No. 4 (June 1965), 465–475.

[TO] J. TATE AND F. OORT, Group schemes of prime order, *Ann. Sci. Ecole Norm. Super (4)* **3** (1970).

[U] R. G. UNDERWOOD, "Hopf Algebra Orders over a Complete Discrete Valuation Ring, Their Duals, and Extensions of R-Groups," doctoral dissertation, State University of New York at Albany, 1992.

[W] W. C. WATERHOUSE, "Introduction to Affine Group Schemes," Springer-Verlag, New York, 1963.

[We] E. WEISS, "Algebraic Number Theory," Chelsea, New York, 1963.